# Лабораторная работа №6

Разважный Георгий НПИбд-02-19

# Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinx на практике совместно с веб-сервером Apache.

# Выполнение лабораторной работы

1. Вошел в систему с полученными учётными данными и убедилась, что SELinux работает в режиме enforcing политики targeted. Обратился с помощью браузера к веб-серверу, запущенному на компьютере, и убедился, что последний работает (рис. 1).

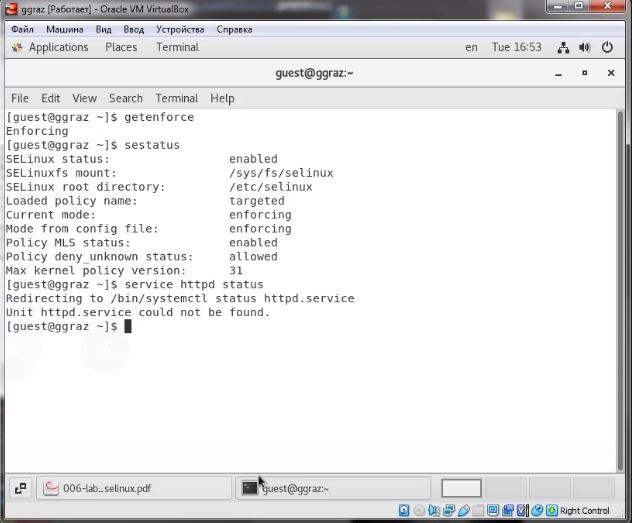


Рис. 1

1. Нашел веб-сервер Apache в списке процессов, определил его контекст безопасности (рис. 2).

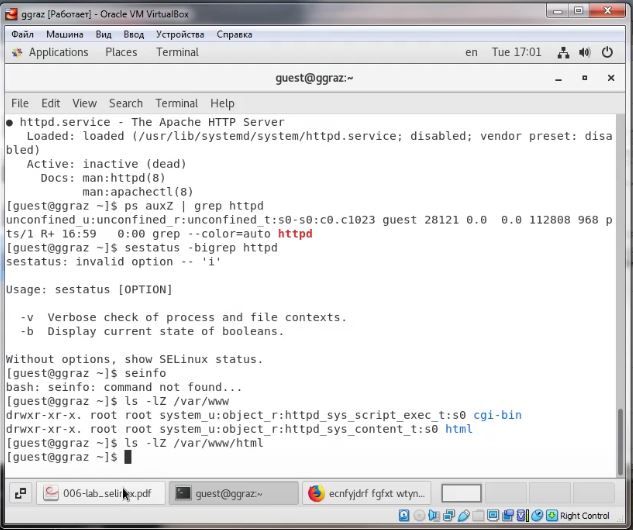


Рис. 2

1. Посмотрел текущее состояние переключателей SELinux для Apache (рис. 3).

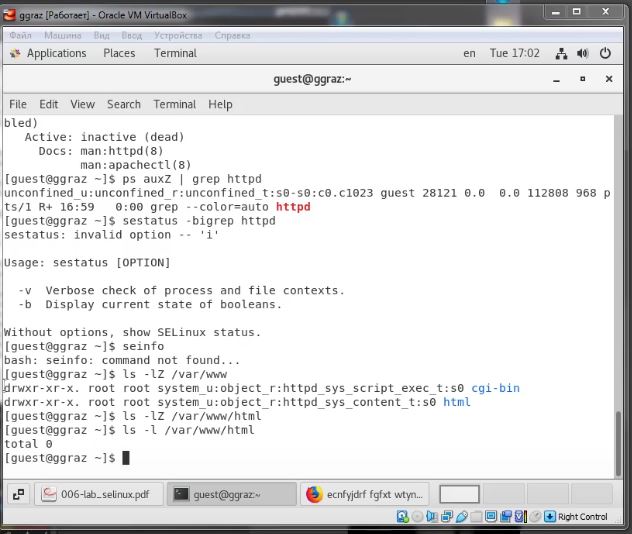


Рис. 3

1. Посмотрел статистику по политике с помощью команды seinfo, также определил множество пользователей, ролей, типов.
2. Определил тип файлов и поддиректорий, находящихся в директории /var/www. Определил тип файлов, находящихся в директории /var/www/html. Определил круг пользователей, которым разрешено создание файлов в директории (рис. 4).

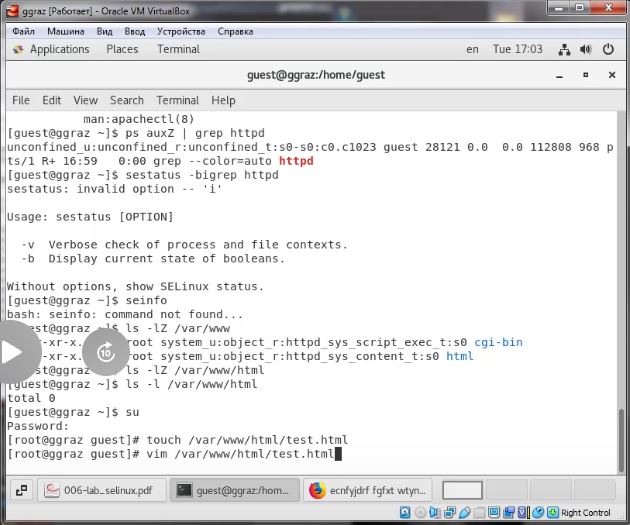


Рис. 4

1. Создал от имени суперпользователя html-файл (рис. 5).

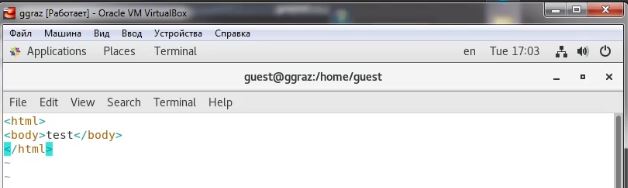
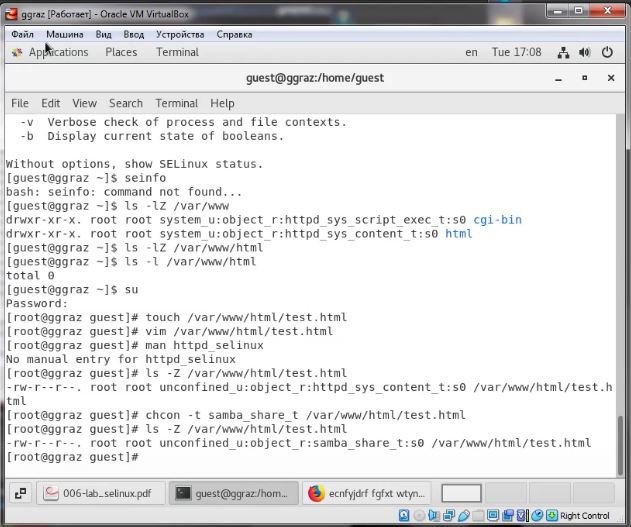
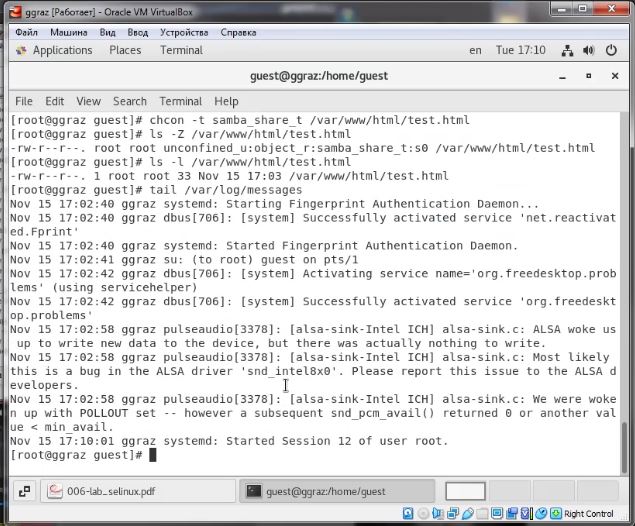
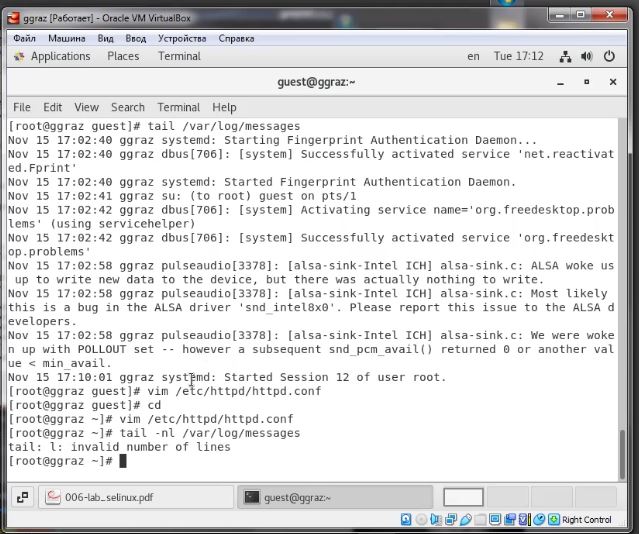
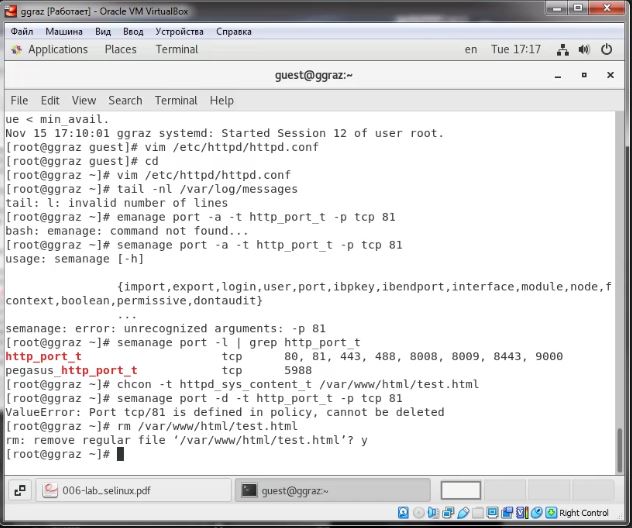


Рис. 5

1. Проверил контекст созданного файла. Контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html: httpd\_sys\_content (рис. 6).
2. Обратился к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html. Убедился, что файл успешно отображён (рис. 7).
3. Изменил контекст файла /var/www/html/test.html с httpd\_sys\_content\_t на samba\_share\_t. После этого проверил, что контекст поменялся (рис. 8). 
4. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес http://127.0.0.1/test.html (рис. 9).
5. Проанализировал ситуацию. Почему файл не был отображён,если права доступа позволяют читать этот файл любому пользователю? Просмотрел log-файлы веб-сервера Apache. Также просмотрите системный лог-файл. Если в системе окажутся запущенными процессы setroubleshootd и audtd, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле /var/log/audit/audit.log. Проверьте это утверждение самостоятельно (рис. 10). 
6. Попробовал запустить веб-сервер Apache на прослушивание ТСР-порта 81. Для этого в файле /etc/httpd/httpd.conf нашёл строчку Listen 80 и заменил её на Listen 81 (рис. 11).
7. Выполнил перезапуск веб-сервера Apache. (рис. 12).
8. Проанализировала лог-файлы. Просмотрела файлы /var/log/http/error\_log, /var/log/http/access\_log и /var/log/audit/audit.log (рис. 13).
9. Выполнила команду semanage port -a -t http\_port\_t -р tcp 81. После этого проверила список портов. Убедилась, что порт 81 появился в списке (рис. 14). 
10. Вернула контекст httpd\_sys\_cоntent\_\_t к файлу/var/www/html/test.html (рис. 15).
11. Исправила обратно конфигурационный файл apache, вернув Listen80.
12. Удалила привязку http\_port\_t к 81 порту. Удалила файл /var/www/html/test.html (рис. 16). 

# Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinx на практике совместно с веб-сервером Apache.